NAG-14C

SAFEGUARDING COMSEC MATERIAL AND FACILITIES

UNITED STATES OF AMERICA

DEPARTMENT OF DEFENSE

NOVEMBER 1997

SAFEGUARDING COMSEC MATERIAL AND FACILITIES

FOREWORD

1. The United States of America provides communications security (COMSEC) material to certain of its Allies, in the interest of protecting classified and sensitive unclassified information which is transmitted electrically between military elements of the U.S. and the allied nation and to protect U.S. information which is released to that nation. When accepting U.S. COMSEC assistance, allied nations agree to protect U.S. COMSEC material, and this document prescribes minimal physical security safeguards for accomplishing that.

2. This is a general document, and the physical security requirements associated with U.S. release of particular cryptosystems take precedence over it.

3. Nations to which this document is provided are encouraged to use it as a basis for the preparation of counterpart documents prescribing standards and procedures for protecting COMSEC materials. To facilitate this, and because COMSEC relationships between the U.S. and certain of its allies is classified, the document is drafted to avoid mention of the United States. Recipient nations may substitute their own Foreword for this page. They may also increase the minimum physical security safeguards prescribed herein, to adapt them to their specific requirements, but may not lower such safeguards.

4. This document is effective upon receipt and supersedes NAG-14A or any similar documents which the United States may have provided in the past, e.g., NAG-6A, Rules for Safeguarding COMSEC Material.

5. This document is intended for use by the military elements of the nations to which it is provided. Its dissemination for other purposes, including releases to public news media, is not in the best interests of the United States or its Allies.

6. Definitions for the specialized COMSEC terms used throughout this document are contained in Annex A.

TABLE OF CONTENTS

CHAPTER I

RESPONSIBILITIES FOR SAFEGUARDING COMSEC MATERIAL AND FACILITIES

1001. INTRODUCTION. COMSEC material is a vital element of the national defense, because it provides the basis for protecting all of the important information which must be transmitted electrically. Responsibility for safeguarding COMSEC material and the COMSEC facilities in which it is used extends from the national or military service level, through the local commanders and their COMSEC custodians, to the individuals who are authorized to hold and use the material. Each level must perform its prescribed functions, if the integrity of the COMSEC material is to be maintained.

1002. NATIONAL/MILITARY SERVICE CHIEF COMSEC RESPONSIBILITIES. The COMSEC responsibilities of the national or military service levels include:

a. Establishing and disestablishing COMSEC accounts.

b. Maintaining a COMSEC central office of record (COR) to verify the accuracy of COMSEC account inventories.

c. Ensuring that COMSEC material is properly obtained, distributed, accounted for, installed, operated, safeguarded, and disposed of.

d. Ensuring that COMSEC custodians and users are properly trained to perform their duties with respect to the safeguarding of COMSEC material and facilities.

e. Conducting liaison with representatives of other nations/services in COMSEC matters.

f. Issuing COMSEC-related directives and providing other COMSEC guidance, as necessary, to ensure that effective use is being made of available COMSEC resources.

1003. COMSEC RESPONSIBILITIES OF LOCAL MILITARY COMMANDERS. Ensuring that the COMSEC material which they are authorized to hold is effectively used and adequately safeguarded is among the general management responsibilities of local military commanders. These individuals must be cleared to the level of the most highly classified material held by their COMSEC accounts. Their COMSEC responsibilities include:

a. Appointing and supervising COMSEC custodians and alternate COMSEC custodians.

b. Supervising COMSEC users in the performance of their duties affecting the use, safeguarding, and destruction or disposition of COMSEC material and the secure operations of COMSEC facilities.

c. Planning and exercising procedures for safeguarding COMSEC material in times of natural and man-made emergencies.

d. Prescribing physical security measures to protect unattended crypto-equipment held by their commands.

e. Reporting COMSEC incidents to proper authorities.

1004. GENERAL RESPONSIBILITIES OF COMSEC CUSTODIANS. Each military command, which holds COMSEC material, must maintain a numbered COMSEC account, and appoint a COMSEC custodian to manage and operate that account. COMSEC custodians must be cleared at least to the level of the most highly classified COMSEC material held in their respective COMSEC accounts. Their principal responsibilities are:

a. Receipting for, storing, amending, accounting for, inventorying, and issuing COMSEC material charged to their COMSEC accounts.

b. Training and advising users of the COMSEC material they issue in the security procedures prescribed for its safeguarding and handling.

c. Destroying or transferring COMSEC material which is in excess of requirements, unserviceable, or superseded and submitting routine COMSEC accounting and destruction reports.

d. Drafting reports of COMSEC incidents.

1005. RESPONSIBILITIES OF COMSEC MATERIAL USERS. Maintaining the integrity of COMSEC material is dependent, in large measure, on the actions of individuals who are authorized to hold and use the material in connection with their official duties. Users must be cleared at least to the level of the most highly classified material to which they have authorized access. Their principal COMSEC responsibilities are:

a. Properly safeguarding and using the COMSEC material issued to them or to which they are authorized access.

b. Reporting to proper authorities any detected occurrence,

circumstance, or act which could jeopardize the integrity or security of COMSEC material.

c. Securely destroying superseded COMSEC key, as directed by the COMSEC custodian.

CHAPTER II

COMSEC CUSTODIANS AND ALTERNATES

2001. IMPORTANCE OF COMSEC CUSTODIANS. If the integrity of the vital COMSEC material is to be maintained, each COMSEC custodian must perform his prescribed functions effectively. Military commanders must ensure that this is being done and should appoint as COMSEC custodians persons who are not over-burdened with other duties and responsibilities.

a. Rank. Individuals appointed as COMSEC custodians and alternated must have sufficient rank and experience to appreciate the importance of the position of trust to which they are being appointed.

b. Training. When operationally feasible, COMSEC custodians should be trained to perform their duties, in advance of being appointed. Where circumstances prevent such advance training, every effort should be made to provide the requisite training as soon as possible.

2002. APPOINTMENT. Each local military commander who is responsible for operation of a numbered COMSEC account must formally appoint a commissioned, warrant, or senior non-commissioned officer (or comparable graded civil servant) to serve as the COMSEC custodian and one or more such persons to serve as alternate COMSEC custodian(s).[1] A copy of each such appointment must be provided expeditiously to the national or service COMSEC COR which oversees the COMSEC account.

2003. DETAILED RESPONSIBILITIES OF COMSEC CUSTODIANS. To the degree competent authority may direct, the COMSEC custodian acts for his commander to receive, safeguard, and dispose of accountable COMSEC material charged to the COMSEC account he manages. He is also responsible for maintaining accurate and current accounting records, and for preparing and forwarding required accounting reports. Specific responsibilities of a COMSEC custodian includes:

a. Receipting for accountable COMSEC material received by his account.

---

[1]Although some alternate COMSEC custodians function as assistants to their respective COMSEC custodians, the principal role of the alternate custodian is to serve as acting COMSEC custodian in the custodian's absence.

b. Page-checking accountable COMSEC documents upon receipt and following entry of amendments affecting page replacement, addition, or extraction.[2]

c. Promptly and accurately entering authorized amendments to accountable COMSEC documents.

d. Ensuring that accountable COMSEC material, including that which has been issued for use, is properly stored and handled. (See Annex A for storage criteria.)

e. Maintaining an accurate inventory of accountable COMSEC material charged to the account showing the current location of each item.

f. Conducting required inventories of accountable holdings of the COMSEC account.

g. Issuing required COMSEC items to authorized users and Maintaining accurate records of issues and returns of such items.

h. Instructing users and using location supervisors in the proper storage and handling of COMSEC material.

i. Drafting, testing, and, if necessary, implementing a plan for safeguarding, evacuating, or destroying accountable COMSEC material in times of natural or man-made emergencies.

j. Transferring or destroying superseded, excess, and unserviceable COMSEC material, in accordance with instructions from proper authorities.

k. Drafting reports of physical, cryptographic, and personnel COMSEC incidents.

l. Preparing and submitting required COMSEC accounting reports.

2004. CUSTODIAN ABSENCE. During normal working hours on regular working days, the COMSEC custodian should be present to perform his duties.

a. Temporary Absence. When a custodian is absent from his duty for less than 60 days, the alternate COMSEC custodian assumes his duties.

[2]Protectively packaged COMSEC key must not be opened upon receipt merely for page checking. Such material should be page checked when it is opened immediately prior to use.

b. Protracted Absence. When a COMSEC custodian will be (or has been) absent from his duty station for longer than 60 days, the responsible commander must appoint a new COMSEC custodian.

c. Permanent Absence. In the event of the death, disability, or departure of a COMSEC custodian, the commander must appoint a new custodian and, if necessary, a new alternate custodian. The new custodian and a properly cleared witness must then inventory the accountable holdings of the COMSEC account and must forward a copy of that inventory to the appropriate COMSEC COR for verification. If any unexplained discrepancies are detected during the inventory, they must be reported to proper authority as COMSEC insecurities.

d. Absence of Alternate Custodian. Inventories are not required when alternate COMSEC custodians are changed or are absent from their duty station.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER III

SAFEGUARDING COMSEC KEY

3001. INTRODUCTION. Contemporary cryptosystems may be of the manual, auto-manual, and machine types, and all types are or use "key". Cryptographic security of electrically transmitted information depends on the proper use of unjeopardized key. To ensure the key provided for use is inviolate, it must be carefully safeguarded throughout its existence, from production through secure destruction.

3002. CRYPTO MARKING. "CRYPTO" is a marking used to identify all hard-copy key (e.g., cards, tapes, lists, codes) intended to protect or authenticate telecommunications.[1] The "CRYPTO" caveat is intended to highlight the extraordinary importance of COMSEC key to the national security and to assist in affording it the proper safeguards.

3003. ACCESS. The basic requirement for access to key is strict enforcement of the concept of "need-to-know," which means that no person may be permitted access unless he requires it for effective performance of his official duties. No person is entitled to have access to key solely by virtue of his rank or status.

a. Granting Access. Access to key may be granted by responsible military commanders to persons under their authority whose duties require access and who hold security clearances appropriate for the COMSEC material to which they will be granted access.

b. Access Criteria. Persons who are authorized access to key must have demonstrated unquestioned loyalty, and their character, habits, and discretion must cast no doubt on their trustworthiness.

3004. STORAGE. Unless appropriately cleared persons are using or otherwise safeguarding key, it must be stored in the most secure facilities available. Minimum storage criteria for key may be derived from Annex B.

[1] A relatively small amount of COMSEC key is not designated "CRYPTO." The purpose of that material includes classroom training and bench test. Safeguards for this material are based solely on its classification.

3005. ISSUE AND RETURN. Key may be issued to individuals who require it in the performance of their official duties and to using locations, such as communications centers and command posts. All such issues must be documented, so that the location of each item of key will be continuously known by the COMSEC custodian. Likewise, all transactions wherein items of accountable key are returned to the COMSEC account must be documented, to relieve the person to whom it was issued from responsibility for it.

a. User Security Training. When key is issued to an individual or to a using location, the issuing COMSEC custodian must ensure that the person(s) who will be responsible for its safeguarding understands the requirements for its proper storage and handling. When this has been done, responsibility for safeguarding the material shifts to the person who signs for it.

b. Issue to User Sites. When key is issued to a user location, such as a command post, the person responsible for that location must ensure that a procedure for continuous account-ability is maintained. The normal way of accomplishing this is to have each oncoming supervisor sight and sign for the key (and any other accountable COMSEC material held) in a log or record book. Changes in a user site's COMSEC material holdings should be supervised by the COMSEC custodian.

3006. SUPERSESSION AND ROUTINE DESTRUCTION. Each item of key is recurringly or irregularly replaced and falls, at any given time, into the category of "future," "effective," or "superseded." Of these categories, superseded key is the most valuable to hostile interests seeking to exploit user communications, because it may have already been used to protect important transmissions which they have already intercepted. It is vital to the maintenance of effective communications security that viable procedures be established and enforced for routinely destroying superseded key.

a. Timely Destruction. Destruction of superseded key must be accomplished as soon as possible (i.e., within twelve hours), preferably as part of the rekeying routine, by persons who perform rekeying. The practice of returning superseded key to COMSEC custodians for destruction at a later date is normally far less secure and prone to exploitation by hostile cognizant agents, and should be adopted only when timely user destruction is not feasible. Local military commanders should consider making suitable key destruction facilities (e.g., desktop shredders) available to key using locations, to facilitate timely destruction of key settings (e.g. key tape segments) as they are superseded.

b. Recording Destruction. Careful records of key setting

destructions must be kept, and all such destructions must be witnessed by properly cleared persons. Centrally prescribed or locally devised forms must be used to record user destruction of superseded key settings. Destruction records must be returned to the issuing COMSEC account and retained as proof that secure, witnessed destructions have taken place.

c. Destroying Complete Editions. Key which is not issued to users may be destroyed as entire editions by COMSEC custodians and their assistants, following supersession. Routine destruction of this type must take place within 15 days after the end of the month in which affected key was scheduled to be effective. They must be witnessed by an appropriately cleared person and expeditiously reported to the proper COR, so that the COMSEC account's responsibility for the material may be removed.

3007. INVENTORIES. COMSEC accounts must inventory the key for which they are responsible semiannually and whenever the COMSEC custodian changes. Reports of all such inventories must be expeditiously submitted to the supporting COR for verification.

3008. RECEIVING AND SHIPPING. COMSEC custodians are responsible for inspecting the protective packaging of received key for signs of tampering and for initiating COMSEC insecurity reports if tampering is suspected. Normally, key intended for use at a particular COMSEC account is delivered there, is used, and is destroyed. However, in rare occasions, key must be transferred between COMSEC accounts. If it becomes necessary to transfer key, custodians must ensure that the material is properly prepared for shipment, that authorized means of shipment are used, and that a copy of the transfer report which accompanies each shipment is expeditiously sent to the supporting central office of record.

a. Shipping. Key marked "CRYPTO" must be shipped in the custody of authorized and appropriately cleared couriers who are responsible for ensuring the integrity of the material in their custody, until it is delivered to a final or intermediate destination. Couriers who must leave the local area should be appointed in writing, and should carry copies of their appointments, so that the material they carry will be immune from examination by other government officials, such as police and airport security personnel.

b. Wrapping. Shipments of key must be double-wrapped and securely sealed. Inner wrappings must be marked with the "CRYPTO" caveat and the classification of the most highly classified material contained in the package. Both inner and outer wrappers must show the "TO" and "FROM" addresses and other notations needed to effect delivery. The outer wrapper must not

reveal that a package contains classified information or COMSEC key.

c. Electrical Transmission of Key. Operational key may be transmitted electrically only under emergency conditions (e.g., when routine key resupply is impossible before the material is required), and then only when the communications system being used for the transmission provides end-to-end security at or above the classification of the transmitted key.

d. Protective Packaging. Most key is protectively packaged, as a defense against exploitation by persons who are authorized to handle it in connection with their official duties, but who covertly function as agents of foreign intelligence services or subversive domestic groups. In general, protective packaging must not be removed from key until immediately prior to the use of the key. It is expressly forbidden to remove protective packaging from key for prior page checking purposes.

CHAPTER IV

SAFEGUARDING COMSEC EQUIPMENT

4001. INTRODUCTION. Crypto-equipment is both classified and unclassified; unclassified crypto-equipment is marked "CONTROLLED CRYPTOGRAPHIC ITEM" (CCI). The embodied cryptographic logic of both categories is classified, and both are authorized to protect information of all classifications, provided key of the appropriate classification is used. Physical safeguards are prescribed to protect crypto-equipment in order to:

a. Prevent acquisition of sophisticated crypto-equipment by unauthorized persons who might use it for unauthorized purposes.

b. Deny unauthorized persons the opportunity to tamper with crypto-equipment, so as to render it ineffective as a COMSEC measure.

c. Limit the opportunity for unauthorized persons to know the details of contemporary cryptographic logic or the protection and fabrication techniques employed in crypto-equipment.

4002. ACCESS. CCI crypto-equipment is purchased and the users are authorized total access to it. However, classified crypto-equipment is provided on condition that only cleared citizens of the producing country are allowed internal access and may perform maintenance. Certain of this equipment is fitted with locks or locking bars to inhibit attempted tampering and/or with tamper detection tape to provide a means of detecting such attempts. As is the case with COMSEC key, the basic requirement for access to crypto-equipment is job-related need-to-know.

a. External Access. Access to crypto-equipment may be granted to military and civilian government employees whose duties require access and who posses security clearances equal to or higher than that of equipment or the associated key, whichever is higher. (Keyed equipment assumes the security classification level of the key it contains.)

b. Casual Viewing. Security clearance is not required for casual, external viewing of cryptographic equipment.

4003. STORAGE. When crypto-equipment is not in the possession of, or continuously attended by, an authorized, appropriately cleared person, it must be protected as follows:

a. Uninstalled Classified Equipment. When not installed in an operational configuration (e.g., a ship, aircraft, shelter,

vehicle, backpack, or building), unkeyed classified crypto-equipment must be stored on the basis of its classification.

b. Uninstalled CCI Equipment. When not installed in an operational configuration, unkeyed CCI crypto-equipment must be stored in a manner which affords it protection at least equal to that which is normally provided to other high-value government property and which ensures that access and accounting requirements are maintained.

c. Installed Equipment. When installed in an operational configuration, unkeyed crypto-equipment may be left unattended, provided it is protected to a degree which, in the judgment of the responsible military commander, is sufficient to preclude any reasonable chance of theft, sabotage, tampering, or access by unauthorized persons.

4004. ISSUE AND RETURN. Crypto-equipment may be issued to individuals who require it in the performance of their official duties and to using locations where it is needed. All such issues must be documented, so that the location of each equipment is continuously known to the issuing COMSEC custodian. Returns must also be documented to relieve the person to whom it was issued from responsibility for it.

a. User Safeguarding Responsibilities. When crypto-equipment is issued to an individual or to a using location, the issuing COMSEC custodian must ensure that the person(s) who will be responsible for its safeguarding understands the requirements for proper storage and handling. When this has been done, responsibility for safeguarding the equipment shifts to the person who signs for it.

b. Using Site Supervisor Responsibilities. When equipment is issued to a user location, such as a communications center, the person responsible for that location, or his designee, remains responsible for it, until the equipment is removed by appropriate authority (e.g., the supporting COMSEC custodian). Shift-to-shift inventorying of installed crypto-equipment is not required.

4005. DISPOSITION. Excess or unserviceable crypto-equipment in the classified for unclassified-CCI categories are to be disposed of as follows:

a. Classified Equipment. Classified crypto-equipment which requires repair, or is no longer required, must be returned to the producing country COMSEC account from which it was received.

b. CCI Equipment. CCI crypto-equipment, which is no longer required, must be returned to a national or service cryptorepair facility for destruction; field destruction involves unacceptable

risks. The equipment may be pressed into blocks be means of automobile crushers and the residue disposed as scrap metal. However, the recommended procedure is to remove all components which are marked "CONTROLLED CRYPTOGRAPHIC ITEM" (See the appropriate paragraphs of Annex C) and destroy them by mechanical chopping. The hulks may then be disposed of intact (e.g., sold as surplus government property).

4006. ACCOUNTING. Crypto-equipment must be continuously accounted for, by serial number, to a national or service COR.

a. Inventorying. COMSEC accounts must inventory equipment for which they are responsible upon receipt or transfer, on the occasion of the change of the COMSEC custodian, and at periodic intervals not to exceed one year. Reports of such inventories must be expeditiously submitted to the supporting COR for verification.

b. Inventory Methods. For purposes of periodic and ad hoc inventories, crypto-equipment which is stored or installed locally must be sighted, but hand receipts may be used to verify the continued presence of equipment located at remote sites.

4007. MAINTENANCE. Holders of classified crypto-equipment are not authorized to perform maintenance actions which require extraction of a classified crypto-equipment from its case. However, military and civilian employees of the using nations may connect and disconnect signal and power lines and perform other external actions necessary to exchange an operating unit for an inoperative unit. Holders of CCI crypto-equipment are responsible for maintaining it.

4008. EMERGENCY ACTIONS. Holders of crypto-equipment are authorized to destroy or disable it in times of emergency, when its loss or compromise is imminent. Under such circumstances, the most effective means of destruction is to extract the classified or sensitive components (i.e., those containing the cryptographic logic and alarm functions and which bear either classification or "CCI" markings) and then destroy these elements as thoroughly as conditions permit. The unclassified equipment hulks may then be abandoned in place, without impact on security. (See Chapter VI for detailed emergency destruction guidance, and Annex C for sensitive component identification and removal information.)

4009. SHIPPING AND RECEIVING. COMSEC custodians are responsible for ensuring that crypto-equipment which must be transferred to another COMSEC account is properly prepared for shipment and is transported by authorized means.

a. Transporting Classified Equipment. Classified crypto-equipment must be transported by designated military couriers who are cleared to the level of the equipment being shipped. Such equipment may not be shipped by postal services.

b. Transporting CCI Equipment. CCI crypto-equipment may be transported by any means which affords it protection at least equal to that which is normally afforded to high-value government property and which ensures that access and accounting procedures are maintained.

c. Zeroizing. Crypto-equipment may not be shipped between COMSEC accounts in keyed condition, i.e., each equipment must be "zeroized" before shipment.

d. Suspected Tampering. If a crypto-equipment is received in a container which shows signs of tampering, a COMSEC insecurity report must be sent and the container left unopened until instructions are received from higher authority.

e. Wrapping. Shipments of crypto-equipment must be double-wrapped and securely sealed. The inner wrappings must be marked with the classification or the "CONTROLLED CRYPTOGRAPHIC ITEM" designation, and both inner and outer wrapper must show the "TO" and "FROM" addressees and other notations needed to effect delivery. The outer wrapper must not reveal that a package contains crypto-equipment.

f. Opening for Inventory. Crates and boxes containing crypto-equipment need not be opened solely for inventory purposes. Packing lists or other statements of contents may be accepted as content verification for such containers, until it becomes necessary to open them for other reasons.

4010. CRYPTO-EQUIPMENT AT UNATTENDED SITES. In some situations technical or operational reasons may dictate that crypto-equipment be located at unattended sites. This is permissible under the following safeguards

a. Site Control. The site must be located in an area under firm control, i.e., sufficient military forces must be located in the vicinity to reduce to an acceptable level the risk of covert or overt hostile capture or temporary occupation of the site.

b. Cryptonet Size. Cryptonets whose key is held in equipment at the unmanned site must be kept as small as possible, with unique key used on each communications link, where feasible

c. Key Storage. Uninstalled crypto-equipment and key which is not held in the equipment may not be stored at the site.

d. Guard Force Response. The commander responsible for operation of the unattended site must arrange for timely guard force response to investigate incidents involving threats to the crypto-equipment on the site.

e. Inspections. Inspections of the unattended site must be conducted to verify that the crypto-equipment installed there has not been tampered with.

f. Construction. The site must be of substantial construction, and all of its accesses (doors, windows, vents) must be alarmed to the location of the supporting guard force.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER V

SAFEGUARDING OTHER COMSEC DOCUMENTS

5001. INTRODUCTION. Cryptosystems normally include operating instructions (SAOs for the classified equipments and KAOs for the CCI equipment). In addition, general COMSEC doctrinal publications, such as this book, are furnished to users. Such supporting documents require safeguards as indicated below.

5002. ACCESS. As is the case with other COMSEC material, access to COMSEC supporting documentation must be based on the need-to-know principle, coupled with appropriate security clearance for classified items. Access to such documents may be granted by responsible military commanders to persons whose duties require access and who hold security clearances appropriate for the material to which they will be granted access.

5003. STORAGE. COMSEC supporting documentation should be stored in accordance with the criteria contained in Annex B.

5004. ISSUE. Issues of COMSEC supporting documentation must be recorded, so that the location of each item is continuously known to the issuing COMSEC custodian. The custodian must also ensure that the individuals who assume responsibility for safeguarding such documents understand the prescribed procedures for protecting them.

5005. SUPERSESSION AND ROUTINE DESTRUCTION. When an accountable COMSEC supporting document is authorized for destruction, normally through a statement in the foreword of the document which supersedes it, COMSEC custodians should effect secure destruction of the document by burning, shredding, or pulping it. Destruction must be reported to the supporting COR.

5006. INVENTORIES. Accountable COMSEC supporting documents must be included in the periodic and ad hoc inventories of the COMSEC accounts, which hold them.

5007. RECEIVING AND SHIPPING. Guidance for handling of COMSEC supporting documents is presented below:

a. Page Checking. COMSEC supporting documents should be page checked against their respective lists of effective pages upon receipt, transfer, or destruction, and in connection with the entry of any amendments, which involve page replacement. The

conduct of page checks should be recorded on the "Record of Page Checks" page.

b. Wrapping. Shipments of COMSEC supporting documents must be double-wrapped, with both inner and outer wrappers showing the "TO" and "FROM" addressees, but only the inner wrapping showing the classification, if any.

c. Shipping. COMSEC supporting documents may be shipped by any means authorized for material of their classification.

5008. AMENDMENTS. Changes may be made in COMSEC supporting documentation, by means of messages or printed amendments. When a COMSEC custodian or an assistant enters an amendment to such documents, he must record the fact by completing an entry on the "Record of Amendments" page of the document.

CHAPTER VI

ROUTINE DESTRUCTION AND EMERGENCY PROTECTION OF COMSEC MATERIAL

6001. PURPOSE. This chapter prescribes standards for the routine destruction of COMSEC key and supporting documentation and provides criteria and guidance for the protection of COMSEC key, equipment, and supporting documentation under emergency conditions.

6002. ROUTINE DESTRUCTION.

a. Destruction Policy. The security achieved through the proper use of cryptosystems is heavily dependent upon the physical protection, which is afforded the associated key. Superseded and current key is extremely sensitive, since its compromise potentially exposes to compromise all information encrypted in the affected systems. For this reason, key must be securely destroyed as soon as possible after it has been superseded or has otherwise served its intended purpose. Likewise, timely destruction of excess or superseded supporting COMSEC documents is important to the national security. Routine destruction of classified and CCI COMSEC equipments and components is not authorized. Classified COMSEC equipment which is unserviceable or which is no longer required must be forwarded through appropriate channels to a COMSEC account of the providing country (normally the account from which it was received). Destruction of unserviceable or unneeded CCI equipment is a responsibility of the purchasing nation; see paragraph 4005.b.

b. Routine Destruction Procedures. Routine destruction of key and supporting documentation may be done by actual users where feasible, or by the COMSEC custodian and a properly cleared witness.

c. Scheduling Routine Destruction.

(1) Key which has been issued for use must be destroyed as soon as possible after supersession, preferably as part of the rekeying routine, and may not be held longer than 12 hours following supersession. However, where special circumstances prevent compliance with the 12-hour rule (e.g., the incinerator is not operational over a weekend or holiday), local commanders or responsible officials may grant extensions of up to 24 hours.

(2) Complete editions of superseded key which are held

at COMSEC accounts must be destroyed within 15 days after supersession.

(3) Superseded supporting COMSEC documents held at COMSEC accounts should be destroyed within 15 days after supersession.

(4) Residue of entered amendments to COMSEC documents must be destroyed within 15 days after entry of the amendment.

d. Routine Destruction Methods. Authorized methods for routinely destroying paper COMSEC material are burning, pulverizing or chopping, crosscut shredding, and pulping.

(1) When destroying paper COMSEC material by burning, the combustion must be complete, so that all material is reduced to ash. Combustion must be contained so that no unburned pieces escape, and ashes must be inspected and, if necessary, broken up or reduced to sludge.

(2) When pulping, pulverizing, or chopping devices are used to destroy paper COMSEC material, it must be reduced to bits no larger than five millimeters in any dimension.

(3) When crosscut (double cut) shredders are used to destroy paper COMSEC material, it must be reduced to shreds not more than 1.2 mm in width and not more than 13 mm in length or not more than 73 mm in width and not more than 22 mm in length.

e. Approving Routine Destruction Devices. Approving devices used to destroy COMSEC material is the responsibility of the head of the using service. Such approval should be withheld until a device has been demonstrated to meet the standards expressed in this chapter. Another consideration in selecting and approving devices for routine destruction is their usefulness in event of emergency destruction. Devices which require long, complicated setup or make-ready procedures should be avoided, as should devices which are incapable of extended full-capacity operation.

f. Reporting Routine Destruction. At least monthly, the COMSEC custodian for each COMSEC account must report the routine destruction of accountable COMSEC aids to its COR, in accordance with procedures prescribed by its service. When accountable paper COMSEC materials are destroyed by their users, local destruction records must be furnished to the supporting COMSEC custodian, as a basis for his reporting their destruction to the COR.

6003. EMERGENCY PROTECTION OF COMSEC MATERIAL.

a. Emergency Protection Planning. Each activity, which holds cryptosystems, must maintain a current, written emergency plan for the protection of such material during manmade disasters (e.g., war or riot) and natural catastrophes (e.g., fire or typhoon). For natural disasters, planning should be directed toward security control over the material until order is restored. By contrast, planning for hostile actions should concentrate on actions to safely evacuate or securely destroy the COMSEC material. Operating routines for COMSEC facilities should be structured so as to minimize the number and complexity of actions which must be taken during emergencies to protect COMSEC material, e.g., routine destruction should be conducted frequently and excess COMSEC material routinely disposed of, so that only minimum amounts of such material are held, and COMSEC material should be stored in ways which will facilitate emergency evacuation or destruction, under emergency conditions.

b. Preparedness Planning For Disasters. Disaster planning must provide for:

(1) Fire reporting and initial fire fighting by personnel assigned to the COMSEC facility.

(2) Assignment of on-the-scene responsibility for ensuring protection of the COMSEC material held.

(3) Securing or removing COMSEC material and evacuation of the endangered area.

(4) Protection of COMSEC material when admission of outside fire fighters and medical or rescue workers into the COMSEC facility.

(5) Assessment and reporting of probable exposure of COMSEC material to unauthorized persons during the emergency.

(6) Post-emergency inventory of COMSEC material and reporting of any losses or unauthorized exposure to appropriate authority.

c. Preparedness Planning for Hostile Actions. Planning for hostile actions must take into account the possible types of situations which may occur, e.g., an orderly withdrawal over a specified period of time, a hostile environment situation where destruction must be carried out in a discrete manner to avoid triggering hostile actions, or fully hostile imminent overrun

situations. Such planning must assess the threat that various types of hostile actions will occur at the affected COMSEC facility and the jeopardy, which these potential emergencies pose to the COMSEC material, held. Emergency action plans must provide for:

(1) Adequate physical security protection capabilities, e.g., perimeter controls, guard forces, and physical defenses, at the individual buildings and other locations in which COMSEC material is held.

(2) Facilities for effecting emergency evacuation of jeopardized COMSEC material under emergency conditions. (Under most circumstances, COMSEC key should be destroyed rather than evacuated.)

(3) Facilities and procedures for effecting secure emergency destruction of COMSEC material held, including adequate supplies of destruction devices, availability of electrical power, secure nearby storage facilities, adequately protected destruction areas, personnel assignments, and responsibilities for directing implementation of emergency destruction.

(4) Precautionary destruction of COMSEC material, particularly superseded and future key which is not operationally required to ensure continuity of operations during the emergency.

d. Establishing Emergency Communications. External communications during emergency situations should be limited to contact with a single remote point, which will act as a distribution center for outgoing messages and as a filter for incoming queries and guidance, thus relieving personnel at the jeopardized site from multiple actions during emergency situations. In situations where over-run is imminent, secure communications should be discontinued in time to allow for thorough destruction of all COMSEC material.

e. Drafting an Emergency Plan. The emergency plan for a particular COMSEC facility should normally be prepared by the COMSEC custodian, but the responsible military commander must be aware of an approved plan. If the plan calls for destroying the COMSEC material, all destruction material, devices, and facilities must be readily available and in good working order. Duties under the plan must be clearly described, and personnel assigned such duties must be trained to perform them effectively. Training exercises should be conducted at least quarterly, to ensure that the emergency plan can be expeditiously implemented. The three options available in an emergency affecting the security of COMSEC material are securing the material within the facility, removing it from the scene of the emergency, and destroying it. Planners must consider which of these apply at

their facilities, either singularly or in combination. When to choose each option should be clearly stated in the plan. For example, if it appears that a civil uprising will be of short duration and the COMSEC facility will soon be reoccupied, the appropriate action might be to destroy superseded key, evacuate effective and future key, remove sensitive elements from crypto-equipment (see Annex C) and lock them, along with classified COMSEC documents, in a safe or vault, secure the facility doors, and leave.

f. Emergency Destruction Priorities. Three broad categories of COMSEC material which may require destruction in emergencies are key, supporting documentation, and equipment. Priorities for destroying these material are:

(1) Superseded, effective, and future key, in that order.

(2) Sensitive elements from crypto-equipment; see Annex C.

(3) Remaining classified COMSEC materials, e.g., operating instructions.

g. Emergency Destruction Tools. Hand tools, such as hammers, screwdrivers, pliers, crowbars, and sledgehammers, should be readily available for emergency destruction of crypto-equipment. Additionally, sites, which maintain incinerators or pyrotechnics for emergency destruction, should also have tongs and asbestos gloves available.

h. Emergency Destruction Methods. Any of the methods approved for routine destruction of COMSEC material may be used for emergency destruction. In addition, incendiaries and some nonincendiary devices may be effective in emergencies. Guidance for destroying COMSEC material is presented below:

(1) Key and supporting COMSEC documents must be destroyed beyond reconstruction. Any approved paper destruction device will accomplish this. Destruction of paper COMSEC materials may also be accomplished by burning in an incinerator or a pierced metal drum fitted with a screen to prevent disbursement of unburned pieces.

(2) Under actual emergency circumstances, all agreed restrictions on foreign access to the interior of crypto-equipment are waived, in the interest of protecting the equipment from compromise by hostile interests. Under such circumstances, locks and locking bars may be forcibly removed and tamper tape disregarded. Sensitive components of the crypto-equipment must be removed and destroyed as thoroughly as time permits. The

equipment hulks may then be abandoned. If approved incendiary devices are not available for destroying the crypto-equipment sensitive components, less effective emergency destruction may be accomplished with hand tools. For example, printed circuit boards may be chopped with a fire ax and the pieces scattered.

i. Emergency Destruction in Aircraft. In an aircraft emergency, there will normally be little time to destroy COMSEC material. However, all reasonable efforts must be made to prevent the material from becoming accessible to unauthorized persons. Considering such factors as the type and amount of COMSEC material carried, the area of operations and prevailing political situation, and the type of aircraft, emergency destruction procedures must be developed under the following guidelines:

(1) When the aircraft is operating over water and a forced landing is imminent, COMSEC equipment should be zeroized and keying material torn up and dispersed. If feasible, sensitive components should be removed from crypto-equipment and dispersed.

(2) If an emergency landing in friendly territory is imminent, the crypto-equipment should be zeroized, but all COMSEC material should be kept on board the aircraft. However, if the aircraft is being forced or is shot down over hostile territory, the crypto-equipment should first be zeroized. The key should then be torn up and dispersed, and reasonable efforts should be made to remove, smash, and disperse the sensitive components of the crypto-equipment.

j. Emergency Destruction Aboard Ship. If a ship is in imminent danger of sinking in friendly-controlled waters, all crypto-equipment must be zeroized. If time permits, sensitive components should be removed from all crypto-equipment and destroyed. Any COMSEC material which cannot be securely destroyed should be locked in security containers and allowed to sink with the ship. If the ship is in imminent danger of capture or of sinking in an area where foreign salvage is possible, crypto-equipment must be zeroized, all key destroyed, and critical components removed from crypto-equipment and destroyed as thoroughly as possible. Undestroyed or partially destroyed COMSEC materials must be jettisoned, with paper items being first placed in weighted bags.

k. Reporting Emergency Destruction. Accurate information relative to the details of all emergency destructions is absolutely essential for evaluating the security impact of each incident and is second in importance only to the conduct of thorough secure destruction. The commander responsible for safeguarding the COMSEC material, which has been jeopardized, is

responsible for reporting the attendant facts to the appropriate military commander. Reports of emergency destruction must identify the material destroyed, the method(s) of destruction, and the extent of destruction. They must also identify any items of COMSEC material which were not thoroughly destroyed and which may be presumed to be compromised. (See Chapter VIII for detailed guidance for COMSEC insecurity reporting.)

CHAPTER VII

SAFEGUARDING COMSEC FACILITIES

7001. PURPOSE. This chapter prescribes standards for safeguarding secure telecommunications facilities and other locations, which contain COMSEC material. The principal threats, which these standards must defend against, are unauthorized access to or tampering with COMSEC material and copying of key by hostile cognizant agents. (See Annex A for definitions of terms.)

7002. SAFEGUARDING FIXED COMSEC FACILITIES. This paragraph applies to fixed facilities, which contain crypto-equipment and which are devoted principally to activities involving communications, e.g., secure telecommunications and COMSEC facilities. Standards for safeguarding mobile and transportable COMSEC facilities are addressed in paragraph 7003.

a. Location. A fixed COMSEC facility should be located in an area which provides positive control over access and as far as possible from areas which are difficult or impossible to control (e.g., public parking lots, ground floor exterior walls).

b. Construction. A fixed COMSEC facility must be constructed of solid, strong materials, to prevent unauthorized penetration and to show evidence of attempts at unauthorized penetration. It must also provide adequate sound attenuation, so that activity within will not divulge classified or sensitive information through the walls, doors, windows, floors, ceilings, or air vents/ducts. Walls must run from true floor to true ceiling, unless intrusion detection systems are installed to give warning of attempted access to the area above the false ceiling. Only one door should be regularly used for access to the facility. Doors must remain closed when the facility is in operation, except to admit authorized persons. Doors must have sufficient strength to resist forced entry and must be hung so that their hinge pins cannot be removed from outside. COMSEC facilities should not normally contain windows. Where windows exist, they must be secured in a permanent manner, to prevent them from being opened and must be alarmed and/or barred, to prevent their use as access points. Windows must also be covered, painted, or screened, to prevent observation of activity in the COMSEC facility from outside. Additionally, air vents, ducts, or similar openings which breach the walls, floor, or ceiling of the facility must be appropriately secured, to prevent penetration, and equipped with acoustical baffles.

c. Facility Approvals and Inspections. Each COMSEC facility must be approved by the responsible service COMSEC authority before it may hold crypto-equipment, key, and other COMSEC material. Aperiodic inspections must also be conducted, to ensure that a satisfactory COMSEC posture is maintained.

(1) Approval to hold COMSEC material is based on an inspection which determines that the facility meets prescribed physical safeguards, as specified in this document, or in service implementing documents. After initial approval, each COMSEC facility must be reinspected at intervals of no greater than 18 months. A facility must also be reinspected and approved, when there is evidence of penetration or tampering, after alterations, which significantly change the physical characteristics of the facility, when a facility is relocated, or when a facility is reoccupied after being temporarily abandoned.

(2) Secure telecommunications facilities require general COMSEC inspections prior to activation and at intervals not greater than 18 months thereafter. As a minimum, these inspections should cover secure operating procedures and practices, handling and storage of COMSEC material, the emergency plan, and both routine and emergency destruction capabilities and procedures.

(3) In each continuously-manned COMSEC facility, a security check must be made at least once every 24 hours. This need only be a visual check to ensure that all accountable COMSEC material is properly safeguarded and that physical security protection systems and devices (e.g., door locks and vent covers) are functioning properly. In facilities which are not continuously manned, the security check must be conducted prior to departure of the last person and must include additional checks to ensure that the facility entrance door is locked and that installed intrusion detection systems are activated.

d. Access Restrictions and Controls.

(1) Unescorted access to COMSEC facilities must be limited to individuals whose duties require such access and who are appropriately cleared, i.e., cleared for the highest classification of COMSEC material held therein. Normally, these persons have duty in the facility or are in its immediate supervisory chain, and their names appear on an approved access list, which is posted inside the facility. Official visitors who are appropriately cleared and whose duties require admittance, may be granted unescorted access by the responsible commander. All such visits shall be recorded in the visitor register.

(2) Uncleared and other official visitors may be authorized admittance by the responsible military commander,

provided effective security precautions are taken to preclude unauthorized access to classified information. Each such visitor must be under continuous escort by an individual whose name appears on the access list, and all such visits must be recorded in the visitor register.

(3) A visitor record must be maintained at the entrance to each COMSEC facility, to record the arrival and departure of authorized visitors. This register should contain the date and time of arrival and departure, the printed name and signature of the visitor, the purpose of visit, and the signature of the individual authorizing the admittance of the visitor. Visitor registers must be retained for at least one year.

e. Standard Operating Procedure (SOP). Each fixed COMSEC facility must have a written SOP containing provisions for the secure conduct of facility operations and for the safeguarding of COMSEC material. For example, the SOP should include procedures for cryptographic operations, local accountability for COMSEC material used, obtaining COMSEC maintenance support for crypto-equipment, and restricting access, storage, routine and emergency destruction of COMSEC materials, and COMSEC incident reporting. As an adjunct to its SOP, each facility must have an emergency plan.

f. Protection of Lock Combinations. The following requirements apply to combination locks used with COMSEC facility doors and security containers used to hold COMSEC material.

(1) Lock combinations may only be changed by cleared persons having need-to-know for the information safeguarded by the lock. Combinations must be changed when the lock is initially placed in use, when any person having authorized knowledge of the combination no longer requires such knowledge, when the combination is or may have been subjected to compromise, and at least annually.

(2) Recorded lock combinations must be classified the same as the highest classification of information protected by the corresponding locks and must be sealed in opaque envelope for storage in support of the COMSEC emergency plan.

(3) Access to combinations to locks used to protect COMSEC material must be limited to individuals who are authorized access to the material. Where a container is used to store future editions of key, access to its combination must be limited to the COMSEC custodian and alternate custodian(s). Where this restriction cannot be applied because others must have access to the container for current key or other material, future editions of key must be stored separately in a locked strongbox which can

be opened only by the COMSEC custodian or alternate custodian(s), and which must be kept in the security container.

(4) To provide ready access to secured COMSEC material in emergencies, a central record of lock combinations must be maintained in a security container approved for storage of the highest classified combination. Access to the combination to that container must be restricted to persons with proper clearance and need-to-know.

(5) Personnel who require access to COMSEC storage container lock combinations must memorize them. It is expressly prohibited for individuals to record the combinations to locks which protect COMSEC material under any other circumstances than in the sealed envelopes used to protect the copies held for emergency use. Such combinations may not be stored in electronic form in computers.

7003. SAFEGUARDING MOBILE COMSEC FACILITIES.

This paragraph expresses requirements for safeguarding transportable and mobile COMSEC facilities. (See Annex A for definitions of terms.)

a. Approvals and Inspections. Formal approval of transportable and mobile telecommunications facilities is not required, and the only inspection requirement for such facilities is the daily security check to ensure that all COMSEC material is properly safeguarded and that physical security protection systems and devices (e.g., door locks and vent covers) are functioning properly. However, if a mobile COMSEC facility remains operational in a fixed location for six months or longer, it is to be considered a fixed facility and the requirements for facility approvals and inspections, as specified in paragraph 7002.c., above, apply.

b. Access and Controls.

(1) Unescorted access to mobile telecommunications facilities must be limited to appropriately cleared persons whose duties require access.

(2) Uncleared visitors and other persons whose duties do not require regular access may be authorized admittance to mobile telecommunications facilities by responsible authority, provided effective security precautions are taken to preclude unauthorized access to classified and sensitive information. Such visitors must be under continuous escort by a person who is authorized unescorted access.

(3) Mobile telecommunications facilities must maintain access lists and visitor registers as prescribed in paragraph 7002.d, above.

c. Protection of Unattended Facilities. When a mobile COMSEC facility is left unattended for any period of time, it must be secured and guarded, to protect against unauthorized access. Because of the many variations in these facilities (e.g., vans, aircraft, open vehicles), standardized securing criteria cannot be prescribed. In general, where a facility is contained in a solid enclosure (e.g., van or equipment shelter), all access points other than the entrance door must be secured from inside the facility, and the entrance door must be secured with a combination padlock. Where this is not practicable (e.g., in a open vehicle or aircraft) a locking bar or other locking device should be used to prevent removal or tampering with the crypto-equipment. Additionally, unattended mobile COMSEC facilities containing COMSEC material must be guarded by appropriately cleared guards who are either stationed at the entrance to the facility or who make frequent rounds in its vicinity.

d. Protection of Lock Combinations. The combinations to locks used to safeguard transportable or mobile COMSEC facilities or COMSEC material stored therein must be protected in accordance with paragraph 7002.f, above.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER VIII

REPORTING COMSEC INCIDENTS

8001. PURPOSE. This chapter prescribes standard's for reporting COMSEC incidents, to ensure that all detected occurrences affecting COMSEC material are reported promptly to designated service or national officials who are responsible for taking action to minimize the security fact of the reported incident. It is important that all persons who are authorized access to COMSEC materials understand that the purpose of COMSEC insecurity reporting is to form a basis for minimizing the security impact of incidents and not to fix blame for them. Reporting must take place freely, without fear of retribution, in the interest of national security. Disciplinary action should be directed only in connection with COMSEC incidents involving espionage, sabotage, falsification of records, or gross negligence in the safeguarding and handling of COMSEC material.

8002. TYPES OF COMSEC INCIDENTS. Reportable COMSEC incidents fall into three general types, "cryptographic", "physical", and "personnel". The operating instructions furnished with each cryptosystem normally specifies the reportable COMSEC incidents associated with the particular system. However, the following general guidance also applies.

a. Cryptographic Incidents. COMSEC incidents of this type normally involve either a crypto-equipment malfunction or an operator error, which reduces a cryptosystem's ability to perform its security function. Examples include use of key which has been compromised or is known to be defective, unauthorized use of key for other than its intended purpose (e.g., using a test key to protect operational communications), unauthorized extension of a cryptoperiod, use of unauthorized operating procedures, use of an equipment known to be defective, tampering with or making an unauthorized modification to a crypto-equipment, or operating an equipment before completing required alarm checks.

b. Physical Incidents. COMSEC incidents of this type normally relate to incidents in which prescribed physical controls are not maintained over crypto-equipment, key, or supporting documents. Included are instances of loss or finding of COMSEC material, unauthorized access to or failure to properly safeguard such material, suspected or confirmed tampering with a crypto-equipment, unauthorized copying of key, incomplete destruction of superseded key or supporting COMSEC documents, or emergency destruction of COMSEC material.

c. Personnel Incidents. COMSEC incidents of this type relate to persons who have been authorized access to COMSEC material and who may have provided COMSEC information to hostile interests. Examples include known or suspected defections, espionage, sabotage of COMSEC material, capture or presumed capture by an enemy, theft of COMSEC material, or deliberate falsification of COMSEC records.

8003. TYPES OF REPORTS.

a. Initial Reports. An initial message report is required for each detected COMSEC incident. If all pertinent facts are included in the initial report, it may also serve as the final report.

b. Amplifying Reports. An amplifying report is required whenever significant new information concerning a reported COMSEC incident is discovered. An amplifying report may also serve as the final report, if it appears likely to the originator that no further information affecting the evaluation of the incident will be determined.

c. Final Reports. A final report is required for each reported COMSEC incident, unless the initial report or an amplifying report served that purpose and so states. Final reports should include summaries of the results of all inquiries and investigations of the reported incident and should state the corrective measures taken or planned to reduce the possibility of recurrence of the incident.

8004. REPORT CONTENT AND HANDLING.

a. Media. COMSEC incident reports must be sent by message, unless it would be faster to deliver them to the action addressee by courier.

b. Classification. COMSEC incident reports must be classified on the basis of their content, but not lower than CONFIDENTIAL.

c. Precedence. Initial and amplifying message report should bear IMMEDIATE precedence if they involve effective key or key scheduled to become effective within 15 days, or if they involve defection, espionage, or sabotage. Such reports should bear PRIORITY precedence if they involve future key scheduled to become effective in more than 15 days, or superseded, reserve, or contingency key. Other initial and amplifying reports and all final reports should be assigned ROUTINE precedence.

d. Addressees. COMSEC incident reports must be addressed

to the service COMSEC authority.

e. Content.

(1) Each COMSEC incident report must state whether it is an initial, amplifying, or final report, and whether it reports a cryptographic, physical, or personnel incident. Each such report must identify the COMSEC material involved and must provide all available details of the incident (e.g., time and duration, location, duties--but not the names--of the personnel involved, and the actions taken or planned to prevent recurrence of the incident).

(2) Each COMSEC incident report should include the reporting commander's assessment of the probability that the affected COMSEC material has been compromised.

(3) If improper use of key or improper operating procedures are involved, give a description of the associated communications activity (e.g., on-line, simplex/half-duplex/duplex, point-to-point/netted key), the operating mode of the crypto-equipment (e.g., clock start, message indicator, traffic flow security), and the general type of traffic involved (e.g., voice/data, operations/logistics/intelligence).

(4) If operational use of malfunctioning crypto-equipment is involved, give the symptoms of the malfunction, the likelihood that the malfunction was deliberately induced, and the volume of traffic involved.

(5) If known or suspected defection, espionage, sabotage, or capture of knowledgeable persons is involved, give the individual's general COMSEC background and the extent of his knowledge of cryptographic principles, a list of the COMSEC material to which the individual has had current access, and whether a counter intelligence investigation has been initiated.

(6) If the incident involves loss of COMSEC material, state the actions being taken to locate the material, the possibility of access by unauthorized persons, the possibility of removal of the material by authorized or unauthorized persons, and the methods of disposal for COMSEC material of that type at the affected facility.

(7) If COMSEC material is discovered outside of authorized control, state the action which caused accountability or physical control to be restored, the possibility of access-surreptitious or otherwise, by unauthorized persons, and the estimated length of time the material was unsecured or out of control.

(8) If the material was received in a package, which has been damaged or shows evidence of tampering, give a description of the evidence of tampering, the means of transmittal, and a description of how the package was stored after receipt. (Do not remove the inner wrapping, until instructions to do so are received from higher authority.)

(9) If the incident involved unauthorized reproduction of COMSEC material, give a complete identification of the equipment or material copied or photographed, the reason for reproduction and how reproduction is controlled at the affected facility, whether espionage is evident or suspected, and the degree to which details of the crypto-equipment, key, or supporting documents were copied or photographed. (If copies of the reproductions are available, forward them separately.)

(10) If tampering with, or removal of a locking bar, lock, or tamper-detection tape is involved, provide a description of the incident, and state when and under what circumstances it may have occurred. Also state whether a counter intelligence investigation has been initiated.

(11) If the incident involves an aircraft crash, state the location of the crash and specify whether it is in friendly or hostile territory or whether the aircraft crashed at sea. Also state whether the aircraft remained largely intact or if wreckage was scattered over a large area, whether the area has been secured and by whom, whether the area has been searched for COMSEC material, and whether recovery efforts have been initiated or are planned for the COMSEC material.

(12) If the material is lost at sea, state the geographical coordinates or the approximate distance and direction from shore, the depth of the water, whether the material was in weighted containers, whether the material was jettisoned or remained with the ship or aircraft, whether foreign vessels were in the immediate area, an opinion as to the possibility of successful salvage operations by unfriendly nations, and whether friendly salvage efforts have been made or are anticipated.

f. Possibility of Compromise. Each COMSEC physical insecurity report must state the opinion of the reporting commander as to whether compromise of the jeopardized material is certain, possible, or impossible, and must state the basis for the opinion expressed.

g. Point of Contact. Each COMSEC insecurity report must state the name (and, if appropriate, the telephone number) of a

person at the reporting command who is prepared to respond to queries from the evaluating authority.

Annexes:
- A - Glossary of COMSEC Terms
- B - Numerical Criteria for Storing COMSEC Material

ANNEX A

GLOSSARY OF COMSEC TERMS

Access	The capability and opportunity to gain detailed knowledge concerning, or to alter information or material. NOTE: A person does not have "access" if an authorized person or physical security controls prevent his obtaining detailed knowledge of, or altering information or material.
Accounting Number	A number assigned to an individual item of material or equipment to facilitate its handling and accounting.
Alternate COMSEC Custodian	The individual designated by proper authority to perform the duties of the COMSEC custodian during the temporary absence of the COMSEC custodian.
Amendment	A correction or change to a COMSEC publication.
Authentication	A security measure designed to protect a communications system against acceptance of fraudulent transmissions or simulation, by establishing the validity of a transmission, message, or originator, or a means of verifying an individual's eligibility to receive specific categories of information.
Authentication System	A cryptosystem or process used for authentication.
Authenticator	The means used to confirm the identity or to verify the

	eligibility of a station, originator, or individual.
Auto-manual Systems (AMS)	A programmable, hand-held crypto-equipment used to perform encoding and decoding functions.
Brevity Code/Brevity List	A non-secure code, which has the sole purpose of shortening messages.
Canister	A type of protective package used for dispensing key in punched or printed tape form.
Central Office of Record (COR)	The office of a department or service which keeps records of accountable COMSEC held by elements subject to its oversight. NOTE: Associated functions performed by CORs include establishing and closing COMSEC accounts, maintaining records of COMSEC custodian and alternate custodian appointments, performing COMSEC account inventories, and responding to queries concerning account management.
Challenge and Reply Authentication	A prearranged procedure whereby one communicator requests authentication of another communicator and the latter establishes his validity by a proper reply.
Ciphony	The process of enciphering audio, resulting in encrypted speech.
Cleared Courier	A duly authorized, cleared (to the level of the information being transported), and a trustworthy person who has been officially designated to transport/carry classified information.

Code	Any system of communication in which arbitrary groups of letters, numbers, or symbols represent units of plain text or varying length. NOTE: Codes may or may not provide security. Common categories are codes used to convert information into a form suitable for communications or encryption, brevity codes which reduce the length of time required to transmit information, codes used to describe of a computer, cryptographic codes used to convert plain text to meaningless combinations of letters and numbers and vice versa.
Code Book	A book or other document containing plan and code equivalents in a systematic arrangement, or a technique of machine encryption employing word substitution.
Code Group	A group of letters or numbers or both in a code system used to represent a plain text word, phrase or sentence.
Code Vocabulary	The set of plain text words, phrases or sentences for which code equivalents are assigned in a code system.
Communications Profile	An analytic model of the communications associated with an organization or activity. NOTE: The model is prepared from a systematic examination, communications content and patterns, the functions they reflect, and the communications security measures applied.

Communications Security (COMSEC)	Measures taken to deny unauthorized persons information derived from government and government contractor telecommunications concerning national security, and to establish the authenticity of such telecommunications. NOTE: Communications security includes cryptosecurity, transmission security, and physical security of COMSEC materials and COMSEC information.
Compromise	The disclosure of information or data to persons not authorized to receive it.
COMSEC Account	An administrative entity identified by an account number, responsible for maintaining accountability, custody, and control of accountable COMSEC material.
COMSEC Account Audit	Examination of the holding, records, and procedures of a COMSEC account to ensure that all accountable COMSEC material charged is being properly safeguarded.
COMSEC Accounting	Procedures, which document the control of accountable COMSEC material from its origin through destruction or final disposition.
COMSEC Aids	All COMSEC material, other than equipment or devices, which assist in securing telecommunications and is required in the production, operation, or maintenance of COMSEC systems and their components.

	NOTE: COMSEC keying material, callsign/frequency systems, and supporting documentation, such as operating and maintenance manuals, are examples of COMSEC aids.
COMSEC Custodian	The individual designated by proper authority to be responsible for the receipt, transfer, accountability, safeguarding and destruction of COMSEC material assigned to a COMSEC account.
COMSEC Device	Synonymous with COMSEC equipment. NOTE: Formerly a COMSEC end item which does not contain a cryptographic algorithm.
COMSEC Doctrine	Rules, procedures, and guidelines for developing, operating and safeguarding COMSEC equipment, systems, and components.
COMSEC End Item	An equipment or combination of components ready for its intended use in a COMSEC application.
COMSEC Equipment	Equipment designed to provide security to telecommunication by converting information to a form unintelligible to an unauthorized interceptor and by reconverting such information to its original form for authorized recipients, as well as equipment designed to aid in, or as an essential element of the conversion process. NOTE: COMSEC equipment includes crypto-equipment, crypto-ancillary equipment, crypto-production equipment, and authentication equipment.

COMSEC Facility	A space that generates, stores, or otherwise contains COMSEC material.
COMSEC Incident	Any uninvestigated or unevaluated occurrence that has the potential to jeopardize the security of COMSEC material or the secure transmission of government information, or any investigated or evaluated occurrence that has been determined as hot jeopardizing the security of COMSEC material or the secure transmission of government information.
COMSEC Information	Information in any form which relates to communications security.
COMSEC Material	COMSEC aids and hardware items which have the purpose to secure telecommunications or to ensure the authenticity of such communications. NOTE: COMSEC material includes but is not limited to, COMSEC key, items, which embody or describe cryptographic logic, and other items, which perform COMSEC functions.
COMSEC Material Control System (CMCS)	A logistic system through which COMSEC material marked "CRYPTO" and other COMSEC material is distributed, controlled and safeguarded. NOTE: The CMCS consists of all COMSEC Central Offices of Records, cryptologistic depots and COMSEC accounts.
COMSEC Module	A removable equipment component that performs COMSEC functions for a

	telecommunications equipment or system.
COMSEC Monitoring	The act of listening to or recording telecommunications transmissions to provide material for analysis, order to determine the degree of security being provided to those transmissions.
COMSEC User	An individual who is required to use and safeguard COMSEC material in the performance of his official duties.
Contingency Key	Key held for use under specific operational conditions or in support of specific contingency plans.
Controlled Area	An area within which uncontrolled movement does not permit access to classified information and which is designed for the principal purpose of providing administrative control, safety, or a buffer area of security for limited access areas.
Controlled Cryptographic Item (CCI)	An unclassified, but controlled secure telecommunications equipment and associated cryptographic assembly, component or other hardware or firmware item that performs a critical COMSEC ancillary or COMSEC function. NOTE: CCIs are married "CONTROLLED ITEM" or, where labeling space.
Controlling Authority (CA)	The official responsible for directing the operation of a cryptonet and for managing the operational use and control of keying material assigned to the cryptonet.

Critical Information	Information, which must be protected from loss and which must be available on a timely basis for effective mission accomplishment.
CRYPTO	A marking or designator identifying COMSEC keying material used to secure or authenticate telecommunications carrying classified or sensitive government or government-derived information, the loss of which could adversely affect the national security interest. NOTE: When written in all upper case letters, "CRYPTO" has the meaning stated above. When written in lower case as a prefix, "crypt" and "crypto" are abbreviations for "cryptographic".
Crypto-alarm	A circuit or device, which detects failures or aberrations in the logic or operation of a crypto-equipment. NOTE: A crypto-alarm may inhibit transmission or may provide a visible and/or audible alarm
Crypto-algorithm	A well defined procedure or sequence of rules or steps, which is used to produce cipher text from plain text and vice versa.
Crypto-ancillary Equipment	Equipment designed specifically to facilitate efficient or reliable operation of crypto-equipment, but which does not perform cryptographic functions.

Crypto-equipment	Equipment, which embodies a cryptographic logic.
Cryptographic	Pertaining to, or concerned with cryptography.
Cryptography	The principles, means, and methods for rendering plain information unintelligible and for recovering encrypted information into intelligible form.
Cryptonet	The stations holding of a specific short title of operational or contingency key. NOTE: Activities, which hold key for other that communications purposes, such as cryptologistics depots, are not cryptonet members.
Cryptoperiod	The time span during which each key setting for a cryptosystem remains in effect.
Cryptosecurity	The security or protection resulting from the proper use of technically sound cryptosystems.
Cryptosynchronization	The process by which a receiving decrypting cryptographic logic attains the same internal state as the transmitting encrypting logic.
Cryptosystem	The associated items of COMSEC material used as a unit to provide a single means of encryption or decryption.
Decipher	To convert enciphered text to equivalent plain text by means of a cipher system.

Decode	Converting encoded text to equivalent plain text by means of a code.
Decrypt	A generic term encompassing decipher and decode.
Electronics Security (ELSEC)	The protection resulting from all measures designed to deny unauthorized persons information of value, which might be derived from the interception, and analysis of non-communications electromagnetic radiations, such as radar.
Element	A subdivision of a COMSEC equipment, or an assembly or subassembly which normally consists of a single piece or group of replaceable parts. NOTE: An element is a removable item necessary to the operation of equipment it does not necessarily perform a complete function in itself.
Encipher	Conversion of plain text to equivalent cipher text by means of a cipher system.
Encode	Conversion of plain text to equivalent encoded text by means of a code system.
Encryption	A generic term encompassing enciphering and encoding.
End-to-end Security	The safeguarding of information in a secure telecommunications system by cryptographic or protected distribution systems means from point of origin to point of destination.
Exercise Key	Key intended for protection of on-the-air transmissions associated with exercises.

Fill Device	A crypto-ancillary device used to transfer or store keys in electronic form or to insert keys into a crypto-equipment.
Fixed COMSEC Facility	A COMSEC facility that is located in an immobile structure or aboard a ship.
Frequency Hopping	The repeated switching of frequencies during radio transmission according to a specified algorithm to avoid unauthorized interception or jamming of telecommunications.
Hand Receipt	A document used to record local or temporary transfer of material from a custodian to a user and acceptance by the user of the responsibility for it.
Hard-Copy Key	Physical keying material such as printed key lists, punched or printed key tapes, or programmable, read-only memories.
High Value Government Property	Items of high monetary or operational value, which require protection against loss or theft. NOTE: A personal computer is an example of high value government property.
Hostile Cognizant Agent	A person who is authorized access to classified or sensitive unclassified information and who intentionally makes it available to a member of a hostile intelligence service or other group whose goals are inimical to the national interest.
Identification Friend or Foe (IFF)	A method of determining the friendly or unfriendly

	character of aircraft, ships, or vehicles, using electronic detection and associated identification equipment.
Intrusion Detection System (IDS)	A system designed to detect and signal the entry of unauthorized persons into a protected area, such as security alarms, sensor systems, video systems.
Inventory Report	A report of items of material that were physically sighted in accordance with COMSEC inventory procedures.
Irregularly Superseded Keying Material	Keying material replace on an "as needed" basis, rather than being replace on schedule.
Key	Information (usually a sequence of random binary digits) used to initially set up and periodically to change the operations performed in a crypto-equipment for the purpose of encrypting or decrypting electronic signals, for determining electronic counter countermeasures patterns (frequency hopping or spread spectrum), or for productivity other keys. NOTE: "Key" has replaced the terms "variable", and "keying variable", and "crypto equipments".
Key Card	A paper card containing a pattern of punched holes which establishes the key for a specific cryptonet at a specific time.
Key Encryption Key (KEK)	Key used to encrypt in the encryption and decryption of other keys for transmission (re-keying) or storage.

Key List	A printed series of key settings for a specific cryptonet.
Key Management	The process by which keys are generated, stored, protected, transferred, loaded, and destroyed.
Keying Material	A type of COMSEC aid which supplies encoding means for manual and auto-manual cryptosystems or key for machine cryptosystems.
Key Stream	A sequence of symbols (or their electrical or mechanical equivalents) produced by a machine or auto-manual cryptosystem to combine with plain text to produce cipher text, to control transmissions security processes, or to produce keys.
Key Tape	Punched or magnetic tape containing key.
Limited Access Area	An area in which uncontrolled movement would allow access to classified information, but in which such access is prevented by escort or other internal restrictions and controls.
Link Encryption	The encryption data in individual links of a communications systems.
Long Title	The descriptive title of an item of COMSEC material.
Machine Cryptosystem	A cryptosystem in which the cryptographic processes are performed by crypto-equipment.
Maintenance Key	Key intended only for off-the-air, in-shop use.

	NOTE: Maintenance key may not be used to protect operational traffic.
Manual Cryptosystem	A cryptosystem in which the cryptographic processes are performed manually without the use of crypto-equipment or auto-manual devices.
Mobile COMSEC Facility	A facility which contains COMSEC material and is configured for operation while in motion.
No-lone Zone	An area, room, or space to which no person may have unaccompanied access and which, when manned, must be occupied by two or more appropriately cleared individuals.
Off-line Cryptosystem	A cryptosystem in which encryption and decryption are performed independently of the transmission and receiving functions.
Operational Key	Key intended for use on-the-air for protection of operational traffic or for the production or secure electrical transmission of key streams.
Page Check	Verification of the presence of each page required in a publication.
Plain Text	Unencrypted information.
Protected Distribution System (PDS)	A wireline or fiber-optics telecommunications system which includes adequate acoustic, electrical, electromagnetic, and physical safeguards to permit its use for the transmission of

	unencrypted classified information.
Protective Packaging	Packaging techniques for COMSEC material which discourage penetration and/or which reveal that a penetration has occurred or which inhibit viewing or copying of keying material prior to the time it is exposed for use.
Regularly Superseded Keying Material	Keying material, which is superseded on a regular established schedule.
Reserve Keying Material	Key held to satisfy unplanned needs.
Risk	The probability that a particular telecommunications system vulnerability will be exploited.
Sample Key	Keys intended for off-the-air demonstration use only.
Secure Communications	Telecommunications, which are effectively secured against hostile exploitation by COMSEC equipment and/or protected distribution systems.
Secure Subscriber Facility	A secure telecommunications facility in which user-operated secure voice, data, facsimile, or video circuits terminate.
Short Title	An identifying combination of letters and numbers assigned to certain COMSEC material for brevity to facilitate handling, accounting, and control.

Signals Security (SIGSEC)	A generic term encompassing communications security and electronic security.
Supersession	Scheduled or unscheduled replacement of a COMSEC aid with a different edition.
Tampering	An unauthorized modification that alters the proper functioning of a COMSEC equipment or system in a manner which degrades the security it provides.
Test Key	Key intended for "on-the-air" testing of COMSEC equipment or systems.
Threat	Any circumstance or event with the potential to cause harm to telecommunications system in the form of destruction disclosure, modification of data, and/or denial of service.
Traffic Analysis (TA)	The study of communications characteristics external to the text.
Traffic Encryption Key (TEK)	Key used to encrypt plain text or to superencrypt previously encrypted text and/or to decrypt cipher text.
Training Key	Cryptographic intended for use for on-the-air or off-the-air training.
Transmission Security (TRANSEC)	That component of communications security, which consists of all measures, designed to protect electrical transmissions from interception and exploitation, by means other than cryptanalysis.
Transmission Security Key (TSK)	A key that is used in the control of transmission

	security processes, such as frequency hopping and spread spectrum.
TSEC Nomenclature	A system for identifying the type and purpose of certain items of COMSEC material. NOTE: TSEC is an abbreviation for telecommunications security.
Two-Person Integrity	A system of storage and handling designed to prohibit access to COMSEC keying material by requiring the presence of at least two authorized persons each capable of detecting incorrect or unauthorized security procedures with respect to the task being performed.
Vulnerability	A weakness in a telecommunications system or system security procedures, hardware design, internal controls, etc., that could be exploited to gain unauthorized access to classified or sensitive information, information handling system, or cryptosystem which is potentially exploitable.
Zeroize	To remove or eliminate the key from a crypto-equipment or fill device.

ANNEX B

NUMERICAL CRITERIA FOR STORING COMSEC MATERIAL

TABLE OF NUMERICAL EQUIVALENTS

Element of Security	Value
Storage Areas	
Security Fences	
Area surrounded by security fence with all gates Secured or controlled	5
Protective Lighting	
Area lighted by protective lighting during hours of Darkness	5
Building or Ship	
Wood frame constructions[1]	5
Controlled area within	15
Limited access area within	25
Exclusion area within	35
No-lone zone manning	50
Masonry or steel construction[1]	10
Controlled	20
Limited access area within	30
Exclusion area within	40
No-lone zone manning	55
Ship, government-owned[1]	25
Controlled area within	35
Limited access area within	40
Exclusion area within	50
No-lone zone manning	60
Storage containers[2]	
Metal locker, keylock (built-in or padlock)	0
Metal locker, combination padlock or high security key padlock	5
Metal locker, high security combination padlock	10
Metal locker, built-in combination lock security container, 10 minute forced entry, 30 minute surreptitious entry	70
Security container, 5 minute forced entry, 20 minute surreptitious entry	60
Security container, no forced entry test requirement, 30 minute surreptitious entry	55

[1] Select only one entry from this category.
[2] Where storage containers are located in vaults, points from both categories may be added.

TABLE OF NUMERICAL EQUIVALENTS
(Continued)

Vaults[2]

Strongroom or weapons magazine	15
Excellent vault, floor, walls, and ceiling 8" thick poured, reinforced concrete; door 10 minute forced entry and 30 minute surreptitious entry; lock three-combination, manipulation-resistant	70
Good vault, floor, walls, and ceiling 6" thick poured, Reinforced concrete; door 10 minute forced entry and 30 minute surreptitious entry; lock three-combination, manipulation-resistant	60
Poor vault, unable to meet one or more of the "good Vault" criteria	50

Guarding

Supporting Guard Force	
Civilian Supporting Guard Force	10
Military Supporting Guard Force	15
Guards	
Civilian guard in general area	10
Civilian guard check of container each hour	15
Civilian guard check of container each half hour	20
Civilian guard in attendance at container	30
Military guard in general area	15
Military guard check of container each hour	20
Military guard check of container each half hour	25
Military guard in attendance at container	60
Sentry dog accompanying military or civilian guard	10

Protective Alarms

Area Alarm System	
Electro-mechanical alarm to detect entry into immediate area	5
Other alarm system to detect entry into immediate area	10
Alarm system to detect attempted entry into immediate area	15
Alarm system to detect attempted entry and approach to immediate area	25
Container Alarm System	
Electro-mechanical alarm to detect opening of container	10
Other alarm system to detect opening of container	15
Alarm system to detect tampering with container	20
Alarm system to detect tampering with and approach to container	25